

Cancer Research And Biostatistics



Supporting the SWOG Statistical Center

SWOG

Leading cancer research. Together.

2011-2012

FISMA* Compliance Assessment

*Federal Information Security Management Act of 2002

**Covering Security for Systems within
Scope of FISMA 2002 Requirements**

Statement of Certification and Accreditation

The undersigned certify that to their knowledge CRAB and SWOG Information Systems and constituent system-level components located at CRAB and within the purview of FISMA 2002 are in compliance. Based on security certifications of systems and supporting evidence provided in the associated security accreditation package (including current system security plan, security assessment report, and plan of action and milestones), the undersigned have determined that risk to information provided by public and private agencies is acceptable. This is formal declaration that security controls have been implemented in the information system and that security meets or surpasses levels of acceptable risk. A summary of recommendations for implementation of additional security controls is attached.

This certification and accreditation of the information system will remain in effect through the next annual renewal period, 2nd quarter of 2012, as long as any vulnerability reported during continuous monitoring processes do not result in unacceptable risk.

Susie Carlin

Susie Carlin, Compliance Manager

30 June 2011

Date

Evonne Lackey

Evonne Lackey, Vice President

June 30, 2011

Date

Keith Goodman

Keith Goodman, Chief Technology Officer

30 June 2011

Date

NIST

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Certification based, in part, upon:

- **Special Publications 800-53 Rev. 3 (August 2009) & 800-53A (July 2009)**
(Recommended Security Controls for Federal Information Systems)
- **FIPS Publications 140-2 (May 2001)**
(Security Requirements for Cryptographic Modules)
- **FIPS Publications 199 (Feb. 2004) & 200 (March 2006)**
(Standards for Security Categorization & Minimum Security Requirements
for Federal Information and Information Systems)
- **Other NIST Publications and Security Analysis Tools**

June 30, 2011

SUMMARY OF RECOMMENDATIONS

1. Information transmitted over the Internet using SWOG's electronic data capture (EDC) system is protected using Secure Socket Layer Version 3.0 (SSL 3.0) encryption. NIST Special Publication 800-52 (June 2005) designates the use of Transport Layer Security Version 1.0 (TLS 1.0) rather than SSL 3.0 for the transmission of qualifying federal data. Additionally TLS 1.0 must use only Federal Information Processing Standards (FIPS) Publication 140-2 (May 2001) approved cryptographic algorithms for its end-to-end network transport layer data encryption. The scope and requirement for use of only 140-2 approved encryption algorithms also extends to the application processing the data, in this case the SWOG EDC system.

Currently SWOG's EDC system does not meet either TLS 1.0 or FIPS 140-2 encryption requirements. Conversion of the SWOG EDC system to meet these requirements is complicated and currently cost prohibitive. SWOG will continue to explore the possible future EDC system conversion to TLS 1.0 and the accompanying FIPS 140-2 encryption but there is no set timeline. In 2012, all new studies are planned to be launched in an NCI-sponsored unified EDC system for all cooperative groups. At that time, FIPS 140-2 compliance will again be reviewed.

2. The disaster recovery/contingency plan should include a business continuity plan for providing staff support as well as restoration of data and applications.
 - Existing disaster recovery processes provide for data backup and recovery within criteria for acceptable risk.
 - A colocation site located in a geologically independent location was established in June, 2011. Planning for the colocation site began in 2010, including review and modification of disaster recovery processes which will take advantage of passive/active servers and storage at the secure facility. Implementation of a business continuity plan to include a strategy for support people will conclude in 2012.